AMENDMENTS TO THE CLAIMS

1-382. (Cancelled)

383. (Currently Amended) A method for routing data objects through a communication network that includes a virus detection system, the method comprising:

classifying an incoming data object to the communication network according to whether said incoming data object includes executable code or does not include executable code ~~a pre-determined criterion related to a type of said incoming data object~~;

if said classifying indicates that said incoming data object includes executable code, ~~is distrusted:~~ routing said incoming data object to the virus detection system; and

if said classifying indicates that said incoming data object does not include executable code, ~~otherwise,~~ routing said incoming data object directly to a destination thereof.~~,~~

~~said criterion being prior information that a data object of said type includes executable code.~~

384. (Previously Presented) The method of claim 383, wherein said incoming data object is selected from the group consisting of a file, a Web page, an e-mail message and a communication packet.

385. (Previously Presented) The method of claim 383, wherein the communication network connects between a wide area network and a local area network.

386. (Previously Presented) The method of claim 383, wherein the communication network connects between a wide area network and a computer system.

387. (Previously Presented) The method of claim 383, wherein the communication network connects between a local area network and a computer system.

388. (Currently Amended) A router apparatus comprising:

computerized virus detection functionality, operative to detect ~~programmable means for detecting~~ viruses within data objects that pass through ~~the~~ said router apparatus;

computerized data object classifying functionality operative to classify ~~programmable means for classifying~~ a data object according to whether said data object includes executable code or does not include executable code ~~a pre-determined criterion related to a type of said data object~~; and

computerized routing functionality ~~programmable means~~, separate from said ~~programmable means for detecting viruses,~~ computerized virus detection functionality, operative to route ~~for routing~~ said data object:

to said computerized virus detection functionality ~~programmable means for detecting viruses~~ if said computerized data object classifying functionality indicates that said data object includes executable code ~~is distrusted~~, and

~~otherwise,~~ directly to a destination of said data object ~~thereof~~ if said computerized data object classifying functionality indicates that said data object does not include executable code.~~,~~

~~said criterion being prior information that a data object of said type includes executable code.~~

389. (Currently Amended) The router apparatus of claim 388, wherein said ~~programmable means~~ computerized virus detection functionality comprises software elements.

390. (Currently Amended) The router apparatus of claim 388, wherein said ~~programmable means~~ computerized virus detection functionality comprises hardware elements.

391. (Currently Amended) A method for routing data objects through a communication network that includes a virus detection system, the method comprising the steps of:

classifying an incoming data object selected from the group consisting of Web pages, e-mail messages and communication packets to the communication network according to whether said incoming data object includes executable code or does not include executable code ~~a pre-determined criterion related to a type of said incoming data object~~;

if said classifying indicates that said incoming data object includes executable code, ~~is distrusted:~~ routing said incoming data object to the virus detection system; and

if said classifying indicates that said incoming data object does not include executable code, ~~otherwise,~~ routing said incoming data object directly to a destination thereof.~~;~~

~~said criterion being prior information that a data object of said type includes executable code.~~

392. (Currently Amended) A router apparatus comprising:

computerized virus detection functionality, operative to detect ~~programmable means for detecting~~ viruses within data objects selected from the group consisting of Web pages, e-mail messages and communication packets that pass through ~~the~~ said router apparatus;

computerized data object classifying functionality operative to classify ~~programmable means for classifying~~ a data object according to whether said data object includes executable code or does not include executable code ~~a pre-determined criterion related to a type of said data object~~; and

computerized routing functionality ~~programmable means~~, separate from said ~~programmable means for detecting viruses,~~ computerized virus detection functionality, operative to route ~~for routing~~ said data object:

to said computerized virus detection functionality ~~programmable means for detecting viruses~~ if said computerized data object classifying functionality indicates that said data object includes executable code ~~is distrusted~~, and

~~otherwise,~~ directly to a destination of said data object ~~thereof~~ if said computerized data object classifying functionality indicates that said data object does not include executable code.~~,~~

~~said criterion being prior information that a data object of said type includes executable code.~~

393. (New) The router apparatus of claim 388, wherein said computerized data object classifying functionality comprises software elements.

394. (New) The router apparatus of claim 388, wherein said computerized data object classifying functionality comprises hardware elements.

395. (New) The router apparatus of claim 388, wherein said computerized routing functionality comprises software elements.

396. (New) The router apparatus of claim 388, wherein said computerized routing functionality comprises hardware elements.